The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/08/2016

SUBJECT:
Cumulative Security Update for Internet Explorer (MS16-142)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer, the most severe of which could allow remote code execution if a user views a specially crafted web page. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
An information disclosure vulnerability (CVE-2016-7199) has been publicly disclosed. There are no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer, the most severe of which that could allow remote code execution. Details of these vulnerabilities are as follows:

- Four memory corruption vulnerabilities exist in the way Internet Explorer accesses objects in memory. (CVE-2016-7195, CVE-2016-7196, CVE-2016-7198, CVE-2016-7241)

- One information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. (CVE-2016-7199)
- One information disclosure vulnerability exists when Microsoft scripting engines improperly handles objects in memory. (CVE-2016-7277)
- One information disclosure vulnerability exists when the Internet Explorer XSS filter is abused to leak sensitive page information. (CVE-2016-7239)

The most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches by Microsoft immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://technet.microsoft.com/library/security/MS16-142

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7195
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7196
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7198
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7199
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7227
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7239
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7241